Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling access to said public key comprising:

denying access to said public key;

providing said recipient with at least one message containing rules of said system, said rules including a rule regarding maintaining secrecy of said public key;

by said recipient, digitally signing said at least one message, by which said recipient agrees to said rules; and

in response to said digital signing, permitting said recipient to utilize said public key.

2. – 17. (Canceled)

18. (Previously Presented) The method of claim 1, wherein said providing includes providing said recipient with a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

19. (Previously Presented) The method of claim 1, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

20. (Previously Presented) The method of claim 1, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

21. (Previously Presented) The method of claim 1, wherein said user transaction is invalid until said digital signing is performed.

22. - 71. (Canceled)

72. (New) The method of claim 1, further comprising:

in response to said signing by said recipient, said certifying authority accepting a transaction from said recipient, said transaction based on said user transaction.

73. (New) A method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising:

denying use of said public key;

providing a recipient with a message containing rules of said cryptographic system, said rules including a rule regarding maintaining secrecy of said public key; and

in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key.

74. (New) The method of claim 73, wherein said providing includes providing said recipient with a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

75. (New) The method of claim 73, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

76. (New) The method of claim 73, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

77. (New) The method of claim 73, wherein a user transaction of said recipient in the system is invalid until said digital signing is performed.

78. (New) The method of claim 73, further comprising:

in response to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system.

79. (New) A method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising:

providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device; and

in response to said recipient digitally signing said message, activating said public key in said secure device.

80. (New) The method of claim 79, wherein said public key is a public key of a certifying authority, said providing is performed by a certifying authority, said digitally signing comprises hashing said message to obtain a hashed document, digitally signing said hashed document to form a digital agreement, and returning said digital agreement to said certifying authority, and said activating is performed by said certifying authority.

81. (New) The method of claim 79, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

82. (New) The method of claim 79, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

83. (New) The method of claim 79, wherein a user transaction by said recipient in the system is invalid until said digital signing is performed.

84. (New) The method of claim 79, further comprising:

in response to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system.

85. (New) A method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising:

said recipient accessing a secure device; and

in response to a predetermined transaction with said secure device, activating said public key in said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device.

86. (New) The method of claim 85, wherein said secure device contains an inactive form of said public key and said activating comprises activating said inactive public key in said secure device.

87. (New) The method of claim 85, wherein said activating comprises transferring said public key to said secure device.

88. (New) The method of claim 85, wherein said public key in said secure device becomes inactive after a certain time period, said method further comprising:

after said public key in said device becomes inactive,

in response to another predetermined transaction with said secure device, activating said inactive public key in said secure device, said other predetermined transaction including

information from the secure device identifying operational capabilities of the secure device and further including information uniquely binding said recipient to said other predetermined transaction.

89. (New) The method of claim 85, where, in said cryptographic system, a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and a user transaction requires verification by a recipient of said user transaction, said verification based on information in a digital certificate and requiring said public key.

90. (New) The method of claim 85, wherein each user of the system has a private key, and wherein said predetermined transaction includes:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

91. (New) The method of claim 85, wherein said predetermined transaction includes a rule to pay for use by said recipient of intellectual property provided through the system.

92. (New) The method of claim 85, wherein a user transaction of said recipient in the system is invalid until said predetermined transaction is performed.

93. (New) The method of claim 85, further comprising:

after said predetermined transaction, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system.

94. (New) A rule system configured to control use by a participant in a cryptographic system of a cryptographic capability, the rule system including one or more rules from the following rules:

a rule regarding maintaining secrecy of the cryptographic capability,

a rule requiring payment upon each use of the cryptographic capability,

a rule requiring payment upon each use of the participant's private key,

a rule requiring payment upon each certification of a certificate's status,

a rule requiring payment for use of intellectual property provided through the cryptographic system, or

a rule requiring payment upon each confirm-to transaction by the participant;

wherein the rule system is configured to make the cryptographic capability available to the participant upon demonstration by the participant of agreement or consistency with the one or more rules.

95. (New) The system of claim 94, wherein the cryptographic capability is expressed as a cryptographic key.

96. (New) The system of claim 95, wherein the cryptographic key is a public key.

97. (New) The system of claim 94, wherein the cryptographic capability is certified by an authority.

98. (New) The system of claim 94, wherein the rule system is configured to make the cryptographic capability available by providing access to an inaccessible cryptographic key.

99. (New) The system of claim 94, wherein the rule system is configured to make the cryptographic capability available by activating an inactive cryptographic key.

100. (New) The system of claim 94, wherein the one or more rules express actions required within the cryptographic system.

101. (New) The system of claim 94, wherein demonstration by the participant of agreement or consistency with the one or more rules is expressed in a message.

102. (New) The system of claim 101, wherein the message comprises the one or more rules.

103. (New) The system of claim 94, wherein the cryptographic capability is provided in a secure device.

104. (New) The system of claim 103, wherein the rule system is configured to make the cryptographic capability available by, in response to demonstration by the participant of agreement or consistency with the one or more rules, transferring the cryptographic capability to the secure device, wherein the cryptographic capability cannot be obtained from the secure device.

105. (New) The system of claim 103, wherein the cryptographic capability in the secure device becomes inactive after a certain time period, the system further comprising:

after the cryptographic capability in the device becomes inactive,

in response to another demonstration by the participant of agreement or consistency with the one or more rules, activating the inactive cryptographic capability in the secure device.

106. (New) The method of claim 94, where, in the cryptographic system, a certifying authority issues digital certificates identifying participants of the cryptographic system, the digital certificates being digitally signed with a private key of the certifying authority to form a digital signature and requiring a public key of the certifying authority in order to verify the digital signature, and a participant transaction requires verification by a recipient of the participant transaction, the verification based on information in a digital certificate and requiring the public key.

107. (New) The system of claim 94, wherein a transaction of the participant in the cryptographic system is invalid until demonstration by the participant of agreement or consistency with the one or more rules.

108. (New) The system of claim 94, further comprising:

a certifying authority configured to accept a transaction from the participant, the transaction based on a transaction of the participant in the cryptographic system, after demonstration by the participant of agreement or consistency with the one or more rules.